STATE OF MARYLAND

MARYLAND STATE RETIREMENT AGENCY (AGENCY)

SMALL PROCUREMENT SOLICITATION

BOARD PORTAL

SOLICITATION NO. SRA 21-05

ISSUE DATE: APRIL 20, 2021

NOTICE TO CONTRACTORS
THIS IS DESIGNATED AS A SMALL PROCUREMENT IN ACCORDANCE WITH COMAR 21.05.07

NOTICE

A Prospective Contractor that has received this document from a source other than eMaryland Marketplace Advantage (eMMA) https://procurement.maryland.gov, should register on eMMA. See **Section 1.3**.

MINORITY BUSINESS ENTERPRISES ARE ENCOURAGED TO RESPOND TO THIS SOLICITATION.

STATE OF MARYLAND
MARYLAND STATE RETIREMENT AGENCY
SOLICITATION KEY INFORMATION SUMMARY SHEET

Small Procurement Solicitation:	**Service: Board Portal**
Solicitation Number:	**SRA 21-05**
Solicitation Issue Date:	**May 12, 2021**
Issuing Office:	**Maryland State Retirement Agency**
Procurement Officer:	**Margie J. Gordon, CPPB** **Maryland State Retirement Agency** **120 E. Baltimore Street, Room 1602** **Baltimore, MD 21202** **Phone: 410-625-5656 Fax: 410-468-1703** **E-mail: procurement@sra.state.md.us**
Contract Manager:	**R. Dean Kenderdine** **Maryland State Retirement Agency** **120 E. Baltimore Street, 16th Floor** **Baltimore, MD 21202** **Phone: 410-625-5600 Fax: 410-468-1703** **E-mail: dkenderd@sra.state.md.us**
Proposals are to be sent to:	**submit Via eMMA**

Proposal Due (Closing) Date and Time: May 26, 2021 at 2:00 P.M. Local Time

Procurement Type:	**Small Procurement**
Contract Type:	**Fixed-Price Contract (per COMAR 21.06.03.03.B (1))**
Contract Duration:	**Two (2) years, starting on or about August 1, 2021, with no renewal options**

Table of Contents

SECTION 1 - GENERAL INFORMATION

1.1 Background and Purpose

1.1.1 Purpose

The Maryland State Retirement and Pension Systems (MSRPS) needs a secure Board Portal for the Agency and MSRPS Board of Trustees (the "Board"). Various Agency personnel are formed into committees, who are responsible for creating, editing, reviewing, and approving documentation that is compiled into a "Board Book" that contains all relevant materials for a particular Board meeting. A Board Book can then be viewed online or printed as hard copy for Board members' use.

The Agency intends to make a single award as a result of this RFP. No portion of the services under this Contract may be subcontracted by the Contractor.

1.1.2 Current Environment

The Board Portal currently in use by various SRA departments and the MSRPS' Board of Trustees is the Directors Desk SaaS. The supported operating systems in use are the most current operating systems, including Microsoft Windows 10. The supported browsers include the most current commercial browsers, including Microsoft Internet Explorer 11.

1.2 Procurement Officer and Contract Manager

The Procurement Officer is the sole point of contact in the State for purposes of this Solicitation prior to the award of any Contract. The name and contact information of the Procurement Officer are indicated in the Key Information Summary Sheet (near the beginning of the Solicitation, after the Title Page and Notice to Vendors). The Agency may change the Procurement Officer at any time by written notice.

The Contract Manager is the State representative for this Contract who is primarily responsible for Contract administration functions after Contract award. The name and contact information of the Contract Manager are also indicated in the Key Information Summary Sheet (near the beginning of the Solicitation, after the Title Page and Notice to Vendors). The Agency may change the Contract Manager at any time by written notice.

1.3 eMaryland Marketplace Advantage

1.3.1 eMMA is the electronic commerce system for the State of Maryland. The IFB, Conference summary and attendance sheet, Bidders' questions and the Procurement Officer's responses, addenda, and other solicitation-related information will be made available via eMMA.

1.3.2 In order to receive a contract award, a vendor must be registered on eMMA. Registration is free. Go to https:/procurement.maryland.gov, click on "Login and Register" under Quick Links to begin the process, and then follow the prompts.

1.4 Questions

1.4.1 All questions shall identify in the subject line the Solicitation Number and Title (SRA 21-05 – Board Portal SP Solicitation), and shall be submitted in writing via e-mail to the Procurement Officer at least five (5) days prior to the Bid due date. The Procurement Officer, based on the availability of time to research and communicate an answer, shall decide whether an answer can be given before the Bid due date.

1.4.2 Answers to all questions that are not clearly specific only to the requestor will be distributed via the same mechanism as solicitation amendments and posted on eMMA.

1.4.3 The statements and interpretations contained in responses to any questions, whether responded to verbally or in writing, are not binding on the Agency unless it issues an amendment in writing.

1.5 Proposals Due (Closing) Date and Time

Proposals must be received by the Procurement Officer at the Procurement Officer's address no later than the Proposal Due date and time indicated in the Key Information Summary Sheet (near the beginning of the Solicitation, after the Title Page and Notice to Vendors) in order to be considered. Requests for extension of this time or date will not be granted.

Contractors may either mail or hand-deliver Proposals. For U.S. Postal Service deliveries, any Proposal that has been received at the appropriate mailroom, or typical place of mail receipt, for the respective procuring unit by the time and date listed in the Solicitation will be deemed to be timely. **Proposals may not be submitted by facsimile.**

1.6 Revisions to the Solicitation

If it becomes necessary to revise this Solicitation before the due date for Proposals, the Agency shall endeavor to provide addenda to all prospective Contractors that were sent this Solicitation or which are otherwise known by the Procurement Officer to have obtained this Solicitation. In addition, addenda to the Solicitation will be posted on https://procurement.maryland.gov.

Failure to acknowledge receipt of an addendum does not relieve the Contractor from complying with the terms, additions, deletions, or corrections set forth in the addendum.

1.7 Cancellations

The Agency reserves the right to cancel this Solicitation.

1.8 Protest/Disputes

Any protest or dispute related, respectively, to this Solicitation or the resulting Contract shall be subject to the provisions of COMAR 21.10 (Administrative and Civil Remedies).

1.9 Mandatory Contractual Terms

By submitting a Proposal in response to this Solicitation, a Contractor, if selected for award, shall be deemed to have accepted the terms and conditions of this Solicitation. Any exceptions to this Solicitation**,** may result in having the Proposal deemed unacceptable, or classified as not reasonably susceptible of being selected for award. **The Agency reserves the right to accept or reject any exceptions.**

1.10 Non-Disclosure Agreement

All Contractors are advised that this solicitation and any resultant Contract(s) are subject to the terms of the Non-Disclosure Agreement (NDA) contained in this solicitation as **Attachment C**. This Agreement must be provided within five (5) Business Days of notification of proposed Contract award; however, to expedite processing, it is suggested that this document be completed and submitted with the Proposal.

1.11 Subcontractors

There will be no subcontracting participation allowed for this Solicitation.

1.12 Small Procurement Designation

The procedures set forth in COMAR 21.05.07 to obtain services for this Solicitation are reasonably expected by the Procurement Officer to cost $50,000 or less.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

SECTION 2 – MINIMUM QUALIFICATIONS

2.1 Contractor Minimum Qualifications

The Contractor must provide proof with its Proposal that the following Minimum Qualifications have been met:

2.1.1 The Contractor shall have no less than three (3) years' experience implementing and maintaining the proposed Board Portals for public pension fund clients that require similar services as those described in this RFP, at least two (2) of which must have been services provided specifically within the last one (1) year. As proof of meeting this requirement, the Contractor shall provide with its Proposal at least three (3) client references for whom the Contractor has provided Board Portals within the past three (3) years, and who are able to attest to the Contractor's experience in providing (specifically) Board Portals to public pension fund clients.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK

SECTION 3 – SCOPE OF WORK

3.1 Scope of Work - Requirements

General Requirements

The Contractor shall:

3.1.1 General Requirements

Provide a secure board portal for the Board with up to 60 users on multiple committees, including at a minimum the following features/capabilities:

A. Electronic access to Board materials, including but not limited to:

1) Storage and filing capability for all Board and committee records;

2) Agenda compilation capability;

3) Board Books, comprised of Board and committee meeting agendas, all supporting documentation for those agendas, and any additional documentation identified for a particular meeting Board Book; and

4) A fully-featured document repository (supporting multiple drafts and final versions) that can be organized for a variety of purposes,

5) Support for document and Board Book level comments and notes, where the meeting packet may be one of any number of collaboration meetings held by committees supporting the Board. Comments must be able to be made by individuals and flagged as private/personal or shared with others. Notes must support board member formal documentation. All notes and comments must be trackable.

B. Collaboration capabilities between the Board Portal users (e.g., trustee support staff), including but not limited to:

1) Electronic member directory of all Board Portal users;

2) Collaboration space containing discussion boards and message threads, including marking discussions as private between certain Board Portal users;

3) Voting capabilities;

4) Survey capabilities;

5) Acknowledgement and approval capture at the individual and committee or the Board-level, as appropriate; and

6) Authorization/approval capture.

C. Calendar function

1) Board calendar showing key dates for the Board;

2) Individual calendars for trustees and other Board Portal users

D. Notifications

1) Email notifications to Board Portal users for calendar entry creation and reminders;

2) New content posting notification

E. User-friendly end-user application

1) Portal shall be accessible using any browser;

2) Simple application and document navigation and straight-forward search capabilities;

3) Mobile and tablet device enabled;

4) Support operating systems, including Microsoft Windows 10, and

5) Supported Browser includes most current commercial browsers, including Microsoft Internet Explorer 11.

F. User-friendly Portal that shall, at a minimum, have the ability to:

1) Upload documents using various Microsoft Office applications

2) Allow edits by authorized users of documents, agendas, and other board materials even after compilation into the Board Book up until point of recording final approval;

3) Allow authorized users to record provisional approval during a meeting with subsequent edits to satisfy the provisional conditions, followed by recording a final approval;

4) Set and control user permissions for all Board Portal capabilities, by both administrators and, where appropriate, by individual users managing meeting materials and documents;

5) Email, print, and share materials from the Board Portal with as few manual steps as possible;

6) Track and control document edits via a log in the production of the Board Books;

7) Publish, edit, and rapidly release documents to all or selected end users, and allow end users to receive materials with as few manual steps as possible; and

8) Prevent editing of any Board materials or committee materials after a vote is registered.

G. Secure environment – the infrastructure environment furnished as part of the Board Portal shall conform to documented industry security standards. Contractor's Board Portal must provide security and privacy features and settings, including but not limited to:

1) SSAE 16 certification

2) Privacy settings on comments, notes, voting, and private discussions

3) The ability to delete documents and annotations, including the ability for certain individuals to edit others' work, where such work includes any feature of the Board Portal.

4) The ability to preclude users, by role or by identified user from accessing certain documents.

5) Multi-level authentication

6) Efficient and secure data backup, where efficiency means the Board Portal is minimally impacted by the backup process.

3.1.2 Provide one-time implementation and configuration services.

3.1.3 Provide end-user training, consisting of:

A. Unlimited web-based Board Portal training for all users

B. Live 1-on-1 administrator and Board member training as needed

C. On-going web training for new Board members and administrators

3.1.4 Provide a 24/7 Help Desk support with 24/7 real-time response.

A. Contractor shall return calls for service within one (1) hour.

3.1.5 Migrate Board materials and data from the current Board Portal

A. Contractor shall work with former board portal provider with data migration format.

3.1.6 Provide a 95% uptime application guarantee, including disaster recovery services.

3.1.7 Contractor-Supplied Hardware, Software, and Materials

A. SaaS applications shall be accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email) or a program interface.

B. The State shall be permitted limited user-specific application configuration settings.

C. The Contractor is responsible for the acquisition and operation of all hardware, software and network support related to the services being provided, and shall keep all software current.

D. All Upgrades and regulatory updates shall be provided at no additional cost.

E. The State requires that the Contractor price individual software modules separately.

F. The Contractor shall provide all documentation for the software furnished under this Contract.

3.1.8 Product Requirements

A. Contractors may propose open source software; however, the Contractor must provide operational support for the proposed software as part of its Proposal.

B. Contractor shall be authorized to furnish the proposed goods and services. Contractors proposing to resell services of another entity must be authorized by such other entity.

C. No international processing for State Data: As described in Section 3.2 Security Requirements, Contractors are advised that any processing or storage of data outside of the continental U.S. is prohibited.

D. Contractors shall clearly indicate which features are part of the base offering and which include additional charges.

E. Consistent expiration dates: A Purchase Order for a service already being delivered to the Agency under this Contract shall terminate on the same calendar day as the prior product/service. As appropriate, charges shall be pro-rated.

F. Any Contract award is contingent on the State's agreement, during the Proposal evaluation process, to any applicable terms of use. Such agreed upon terms of use shall apply consistently across services ordered under the Contract.

G. The Contractor shall not establish any auto-renewal of services beyond the period identified in Contract documents.

H. In addition to any notices of renewal sent to the Agency, Contractors shall email notices of renewal to the e-mail address designated by the Contract Monitor.

I. The Contractor may not modify the functionality or features of any SaaS provided hereunder if such modification materially degrades the functionality of the SaaS.

3.1.9 Maintenance and Support

Maintenance and support, and Contractor's ongoing maintenance and support obligations, are defined as follows:

A. Maintenance commences at the Agency acceptance of initial one-time startup activities. Billing for such maintenance and support shall commence after the Agency accepts the initial one-time implementation and initial training has been completed.

B. Software maintenance includes all future software updates and system enhancements applicable to system modules licensed without further charge to all subscribed users.

C. For the first year, and all subsequent Contract years, the following services shall be provided:

1) Error Correction. Upon notice by the Agency of a problem with the Board Portal (which problem can be verified), reasonable efforts to correct or provide a working solution for the problem.

2) Material Defects. Contractor shall notify the Agency of any material errors or defects in the Board Portal known, or made known to Contractor from any source during the life of the Contract, that could cause the production of inaccurate or otherwise materially incorrect results. The Contractor shall initiate actions as may be commercially necessary or proper to effect corrections of any such errors or defects.

3) Updates. Contractor will provide to the Agency, at no additional charge, all new releases and bug fixes (collectively referred to as "Updates") for any software deliverable developed or published by the Contractor and made available to its other customers.

D. Activity reporting, as available to the SaaS customer base. Any reporting required by the Agency beyond reports generally available to the customer base shall be discussed between the Agency and the Contractor, and may result in additional charges to the Agency.

3.2 Security Requirements

3.2.1 Information Technology

For purposes of this Solicitation and the resulting Contract:

(a) "Sensitive Data" means information that is protected against unwarranted disclosure, to include Personally Identifiable Information (PII), Protected Health Information (PHI) or other private/confidential data, as specifically determined by the State. Sensitive Data includes information about an individual that (1) can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; (2) is linked or linkable to an individual, such as medical, educational, financial, and employment information; (3) falls within the definition of "personal information" under Md. Code Ann., Com. Law§ 14-1305(d); or (4) falls within the definition of "personal information" under Md. Code Ann., State Govt. § 10-1301(c).

(b) The Contractor shall implement administrative, physical, and technical safeguards to protect State data that are no less rigorous than accepted industry standards for information security such as those listed below, and shall ensure that all such safeguards, including the manner in which State data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws as well as the terms and conditions of this Solicitation and resulting Contract.

(c) Contractors shall comply with and adhere to the State IT Security Policy and Standards. These policies may be revised from time to time and the Contractor shall comply with all such revisions. Updated and revised versions of the State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy.

3.2.1.1 Information Security Requirements

To ensure appropriate data protection safeguards are in place, the Contractor shall at a minimum implement and maintain the following information technology controls at all times throughout the life of the Contract. The Contractor may augment this list with additional information technology controls.

(a) Apply hardware and software hardening procedures as recommended by the manufacturer to reduce the Contractor's systems' surface of vulnerability. The purpose of system hardening procedures is to eliminate as many security risks as possible. These procedures may include but are not limited to, removal of unnecessary software, disabling or removing of unnecessary services, the removal of unnecessary usernames or logins, and the deactivation of unneeded features in the Contractor's system configuration files.

(b) Establish policies and procedures to implement and maintain mechanisms for regular internal vulnerability testing of operating system, application, and network devices supporting the services provided under this Contract. Such testing is intended to identify outdated software versions; missing software patches; device or software misconfigurations; and to validate compliance with, or deviations from, the Contractor's security policy. The Contractor shall evaluate all identified vulnerabilities for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly, or document why remediation action is unnecessary or unsuitable. The Agency shall have the right to inspect these policies and procedures, and the performance of vulnerability testing, to confirm the effectiveness of these measures for the services being provided under this Contract.

(c) Where website hosting or Internet access is the service provided, or part of the service provided, the Contractor shall conduct regular external vulnerability testing. External vulnerability testing is an assessment designed to examine the Contractor's security profile from the Internet without benefit of access to internal systems and networks behind the external security perimeter. The Contractor shall evaluate all identified vulnerabilities on Internet-facing devices for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly, or document why remediation action is unnecessary or unsuitable. The Agency shall have the right to inspect these policies and procedures, and the performance of vulnerability testing, to confirm the effectiveness of these measures for the services being provided under this Contract.

(d) Ensure that anti-virus and anti-malware software is installed and maintained on all systems supporting the services provided under this Contract; that the anti-virus and anti-malware software is automatically updated; and that the software is configured to actively scan and detect threats to the system for remediation.

(e) Enforce strong user authentication and password control measures over the Contractor's systems supporting the services provided under this Contract to minimize the opportunity for unauthorized system access through compromise of the user access controls. At a minimum, the implemented measures should be consistent with the most updated and revised versions of the State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy.

(f) Ensure State data under this service is not processed, transferred, or stored outside of the United States.

(g) Ensure that State data is not comingled with the Contractor's other clients' data through the proper application of data compartmentalization security measures. This includes, but is not limited to, classifying data elements and controlling access to those elements based on the classification and the user's access or security level.

(h) Apply data encryption to protect State data, especially Sensitive Data, from improper disclosure or alteration. Data encryption should be applied to State data in transit over networks and, where possible, State data at rest within the system, as well as to State data when archived for backup purposes. Encryption algorithms which are utilized for this purpose must comply with current Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules", FIPS PUB 140-2.

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

(i) Enable appropriate logging parameters on systems supporting services provided under this Contract to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information security events as recommended by the operating system and application manufacturers as well as information security standards including the most updated and revised versions of the State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy.

(j) Retain the aforementioned logs and review them at least daily to identify suspicious or questionable activity for investigation and documentation as to their cause and perform remediation, if required. The Agency shall have the right to inspect these policies and procedures, and the Contractor's performance, to confirm the effectiveness of these measures for the services being provided under this Contract.

(k) Ensure system and network environments are separated by properly configured and updated firewalls to preserve the protection and isolation of Sensitive Data from unauthorized access as well as the separation of production and non-production environments.

(l) Restrict network connections between trusted and untrusted networks by physically and/or logically isolating systems supporting the services being provided under the Contract from unsolicited and unauthenticated network traffic.

(m) Review, at regular intervals, the aforementioned network connections, documenting and confirming the business justification for the use of all service, protocols, and ports allowed, including the rationale or compensating controls implemented for those protocols considered insecure but necessary.

(n) Ensure that the Contractor's personnel shall not connect any of their own equipment to a State LAN/WAN without prior written approval by the State. The Contractor shall complete any necessary paperwork, as directed and coordinated with the Contract Manager, to obtain approval by the State to connect Contractor-owned equipment to a State LAN/WAN.

3.2.1.2 **Incident Response Requirement**

(a) The Contractor shall notify the Contract Manager when any Contractor system that may access, process, or store State data or work product is subject to unintended access or attack. Unintended access or attack includes compromise by computer malware, malicious search engine, credential compromise or access by an individual or automated program due to a failure to secure a system or adhere to established security procedures.

(b) The Contractor shall notify the Contract Manager within one (1) Business Day of the discovery of the unintended access or attack by providing notice, via written or electronic correspondence, to the Contract Manager and Procurement Officer.

(c) The Contractor shall notify the Contract Manager within two (2) hours if there is a threat to the Contractor's systems, as it pertains to the use, disclosure, and security of the Agency's Sensitive Data.

(d) If an unauthorized use or disclosure of any Sensitive Data occurs, the Contractor must provide written notice to the Contract Manager within one (1) Business Day after the Contractor's discovery of such use or disclosure and, thereafter, all information the State requests concerning such unauthorized use or disclosure.

(e) The Contractor, within one (1) Business Day of discovery, shall report to the Contract Manager any improper or non-authorized use or disclosure of Sensitive Data. The Contractor's report shall identify:

1. the nature of the unauthorized use or disclosure;

2. the Sensitive Data used or disclosed;
3. who made the unauthorized use or received the unauthorized disclosure;
4. what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and:
5. what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.
6. the Contractor shall provide such other information, including a written report, as reasonably requested by the State.

(f) The Contractor shall comply with all applicable laws that require the notification of individuals in the event of unauthorized release of PII or other event requiring notification. In the event of a breach of any of the Contractor's security obligations or other event requiring notification under applicable law, the Contractor agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the State and its officials and employees from and against any claims, damages, or other harm related to such security obligation breach or other event requiring the notification.

(g) This Section 3.2.1.2 shall survive expiration or termination of the Contract.

3.3 SOC 2 Type 2 Audit Report

3.3.1 In the event the Contractor provides services for identified critical functions, handles Sensitive Data, or hosts any related implemented system for the State under the Contract, the Contractor shall have an annual audit performed by an independent audit firm of the Contractor's handling of Sensitive Data or the Agency's critical functions. Critical functions are identified as all aspects and functionality of the Board Portal including any add-on modules and shall address all areas relating to Information Technology security and operational processes. These services provided by the Contractor that shall be covered by the audit will collectively be referred to as the "Information Functions and Processes." Such audits shall be performed in accordance with audit guidance: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) as published by the American Institute of Certified Public Accountants (AICPA) and as updated from time to time, or according to the most current audit guidance promulgated by the AICPA or similarly-recognized professional organization, as agreed to by the Agency to assess the security of outsourced client functions or data (collectively, the "Guidance") as follows:

A. The type of audit to be performed in accordance with the Guidance is a SOC 2 Type 2 Audit (referred to as the "SOC 2 Audit" or "SOC 2 Report"). All SOC2 Audit Reports shall be submitted to the Contract Monitor as specified in Section F below. The initial SOC 2 Audit shall be completed within a timeframe to be specified by the State. The audit period covered by the initial SOC 2 Audit shall start with the Contract Effective Date unless otherwise agreed to in writing by the Contract Monitor. All subsequent SOC 2 Audits after this initial audit shall be performed at a minimum on an annual basis throughout the Term of the Contract, and shall cover a 12-month audit period or such portion of the year that the Contractor furnished services.

B. The SOC 2 Audit shall report on the suitability of the design and operating effectiveness of controls over the Information Functions and Processes to meet the requirements of the Contract, including the Security Requirements identified in **Section 3.2**, relevant to the trust principles identified in 3.3.1: as defined in the aforementioned Guidance.

C. The audit scope of each year's SOC 2 Report may need to be adjusted (including the inclusion or omission of the relevant trust services principles of Security, Availability, Processing Integrity,

Confidentiality, and Privacy) to accommodate any changes to the environment since the last SOC 2 Report. Such changes may include, but are not limited to, the addition of Information Functions and Processes through modifications to the Contract, or due to changes in Information Technology or the operational infrastructure. The Contractor shall ensure that the audit scope of each year's SOC 2 Report engagement shall accommodate these changes by including in the SOC 2 Report all appropriate controls related to the current environment supporting the Information Functions and/or Processes, including those controls required by the Contract.

D. The scope of the SOC 2 Report shall include work performed by any subcontractors that provide essential support to the Contractor or essential support to the Information Functions and Processes provided to the Agency under the Contract. The Contractor shall ensure the audit includes all such subcontractors operating in performance of the Contract.

E. All SOC 2 Audits, including those of the Contractor, shall be performed at no additional expense to the Agency.

F. The Contractor shall provide to the Contract Monitor, within 30 calendar days of the issuance of each SOC 2 Report, a complete copy of the final SOC 2 Report(s) and a documented corrective action plan addressing each audit finding or exception contained in the SOC 2 Report. The corrective action plan shall identify in detail the remedial action to be taken by the Contractor along with the date(s) when each remedial action is to be implemented.

G. If the Contractor currently has an annual, independent information security assessment performed that includes the operations, systems, and repositories of the Information Functions and Processes being provided to the Agency under the Contract, and if that assessment generally conforms to the content and objective of the Guidance, the Agency will determine in consultation with appropriate State government technology and audit authorities whether the Contractor's current information security assessments are acceptable in lieu of the SOC 2 Report(s).

H. If the Contractor fails during the Contract term to obtain an annual SOC 2 Report by the date specified in **Section 3.3.1.A**, the Agency shall have the right to retain an independent audit firm to perform an audit engagement of a SOC 2 Report of the Information Functions and Processes utilized or provided by the Contractor under the Contract. The Contractor agrees to allow the independent audit firm to access its facility/ies for purposes of conducting this audit engagement(s), and will provide the necessary support and cooperation to the independent audit firm that is required to perform the audit engagement of the SOC 2 Report. The Agency will invoice the Contractor for the expense of the SOC 2 Report(s), or deduct the cost from future payments to the Contractor.

I. Provisions in **Section 3.3.1-2** shall survive expiration or termination of the Contract. Additionally, the Contractor and relevant subcontractor shall flow down the provisions of **Section 3.3.1-2** (or the substance thereof) in all subcontracts.

3.4 Insurance Requirements

3.4.1 The Contractor shall provide a copy with its proposal of its current certificate of insurance showing the types and limits of insurance in effect as of the Proposal submission date. The Contractor shall maintain Commercial General Liability Insurance with limits sufficient to cover losses resulting from, or arising out of, Contractor action or inaction in the performance of the Contract by the Contractor, its agents, servants, employees, or relevant subcontractors. Any insurance furnished as a condition of the Contract shall be issued by a company authorized to do business in the State.

SECTION 4 – CONTRACT DURATION

4.1 The duration of the Contract will be for a period of two (2) years, with no renewal options.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

SECTION 5 – PROPOSAL FORMAT

5.1 Proposal

5.1.1 Contractor Proposal Response to Solicitation Requirements and Proposed Work Plan

a. The Contractor shall address each RFP requirement (RFP Section 2 and Section 3) in its Proposal and describe how its proposed services, will meet or exceed the requirement(s). If the State is seeking Contractor agreement to any requirement(s), the Contractor shall state its agreement or disagreement. Any paragraph in the Proposal that responds to a requirement found in Section 3 shall include an explanation of how the work will be performed.

b. Implementation Schedule - Contractor shall provide the proposed implementation schedule with its Proposal.

5.1.2 The following documents shall be completed, signed, and included in the Proposal

a. Current Certificate of Insurance
b. SOC 2 Type 2 Audit Report (see Section 3.3)
c. Contractor's Contract

5.2 Two Part Submission

Offerors shall submit Proposals in separate volumes (or envelopes):

- Volume I –Technical Proposal
- Volume II – Financial Proposal

5.3 Proposal Delivery and Packaging

5.3.1 Proposals delivered by facsimile and e-mail shall not be considered.

5.3.2 Provide no pricing information in the Technical Proposal. Provide no pricing information on the media submitted in the Technical Proposal.

5.3.3 Offerors may submit Proposals through the State's internet based electronic procurement system, eMMA.

5.3.4 The Procurement Officer must receive all electronic Proposal material by the Solicitation due date and time specified in the Key Information Summary Sheet. Requests for extension of this date or time will not be granted. Except as provided in COMAR 21.05.03.02F, Proposals received by the Procurement Officer after the due date will not be considered.

5.3.5 Offerors shall provide their Proposals in two separate envelopes through eMMA following the Quick Reference Guides (QRG) labelled "5 - eMMA QRG Responding to Solicitations (RFP)" for double envelope submissions.

5.3.6 Two Part (Double Envelope) Submission:

A. Technical Proposal consisting of:
1) Technical Proposal and all supporting material in Microsoft Word format, version 2007 or greater,

2) Technical Proposal in searchable Adobe PDF format,

3) a second searchable Adobe copy of the Technical Proposal, with confidential and proprietary information redacted (see Section 7, item 5), and

B. Financial Proposal consisting of:

1) Financial Proposal entered into the price form spreadsheet within eMMA and all supporting material in Microsoft Word format, version 2007 or greater format,

2) Financial Proposal in searchable Adobe PDF format,

3) a second searchable Adobe copy of the Financial Proposal, with confidential and proprietary information removed (see Section 7, item 5).

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

SECTION 6 – AWARD BASIS

6.1 The Contract shall be awarded to the responsible Contractor submitting the Proposal that has been determined the most advantageous to the System (see COMAR 21.05.03.03F), for providing the goods and services as specified in this Solicitation.

6.2 The criteria to be used to evaluate each Solicitation Requirement are listed below in descending order of importance.

6.2.1 Contractor's Response to Solicitation Requirements.

The Agency prefers that, in its proposal, a Contractor demonstrate a comprehensive understanding of the Solicitation's work requirements and mastery of the subject matter, including an explanation of how the Contractor will satisfy the work requirements. Proposals which include limited responses to work requirements such as "concur" or "will comply" will receive a lower ranking than those Proposals that demonstrate an understanding of the work requirements and include plans to meet or exceed them.

6.2.2 Contractor Qualifications and Capabilities

6.2.3 Contractor Proposed Price

SECTION 7 – REQUIRED CONTRACT TERMS

For this solicitation, the Contractor is asked to submit its standard form of contract. **A Contractor must be willing to revise its standard form of contract to reflect, at a minimum, the required contract terms below.**

1. The Contract shall include (a) a statement of the scope of the contract that conforms to Section 3 of this RFP (this may be incorporated by reference); (b) the dollar value of the contract, if known or estimated dollar value if the actual value is not known; (c) the term of the contract; (d) names of the procurement officer and contract manager; and (e) a clause containing the following: "The Contractor shall comply with the provisions of State Finance and Procurement Article, Title 19, Annotated Code of Maryland."

2. The Agency will not agree to any indemnification provisions (in which the Contractor is indemnifying the Agency or the System) that allow the Contractor to defend the Agency and/or the System and have sole control over the defense and settlement of any claims against the Agency and/or the System.

3. The laws of Maryland shall govern the interpretation and enforcement of the Contract. Any governing law provision must include that Maryland law will govern the interpretation of Maryland law, regulations, rules, interpretations and directives of the Maryland Office of the Attorney General.

4. Disputes arising under the Contract shall be governed by State Finance and Procurement Article, Title 15, Subtitle 2, Part III, Annotated Code of Maryland, and by Code of Maryland Regulations ("COMAR") 21.10. Pending resolution of a dispute, the Contractor shall continue to perform the Contract, as directed by the Contract Manager.

5. The Agency will not agree to any confidentiality or nondisclosure provisions that create obligations that conflict with the Agency and/or the System's legal obligations under applicable open records laws, including but not limited to the Maryland Public Information Act, Annotated Code of Maryland, General Provisions Article, Section 4-101 to 4-601.

6. The Agency will not agree to provisions that would require the Agency, the System or the State of Maryland to waive any immunity to suit or liability or irrevocably waive sovereign or governmental immunity, or any defenses available to it under Maryland or Federal law. This is not intended as a waiver of a Contractor's right to assert that the contract constitutes a contract within the meaning of Section 12-201, State Government Article, Annotated Code of Maryland, assuming each document is a valid contract under applicable law.

7. The Agency may terminate the Contract, in whole or in part, without showing cause upon prior written notice to the Contractor specifying the extent and the effective date of the termination. The Agency shall pay all reasonable costs associated with the Contract that the Contractor has incurred up to the date of termination and all reasonable costs associated with termination of the Contract. However, the Contractor may not be reimbursed for any anticipatory profits, which have not been earned up to the date of termination. Termination hereunder, including the determination of the rights and obligations of the parties, shall be governed by the provisions of COMAR 21.07.01.12A(2).

8. If the Contractor does not fulfill obligations under the Contract or violates any provision of the Contract, the Agency may terminate the Contract by giving the Contractor written notice of termination. Termination under this paragraph does not relieve the Contractor from liability for any damages caused to the Agency. Termination hereunder, including the determination of the rights and obligations of the parties, shall be governed by the provisions of COMAR 21.07.01.11B.

SOLICITATION ATTACHMENTS

ATTACHMENT A – Financial Proposal Instructions

ATTACHMENT B – Financial Proposal Form
The Financial Proposal Form in a separate excel format must be completed and submitted with the Proposal.

ATTACHMENT C – Non-Disclosure Agreement Forms
This Attachment must be completed and submitted within five (5) Business Days of receiving notification of recommendation for award.

ATTACHMENT A – FINANCIAL PROPOSAL INSTRUCTIONS

In order to assist Contractors in the preparation of their Financial Proposals, and to comply with the requirements of this Solicitation, Financial Proposal Instructions and a Financial Proposal Form have been prepared. Contractors shall submit their Financial Proposal on the Financial Proposal Form in accordance with the instructions on the Financial Proposal Form and as specified herein. Do not alter the Financial Proposal Form, or the Proposal may be determined to be not reasonably susceptible of being selected for award. The Financial Proposal Form is to be signed and dated, where requested, by an individual who is authorized to bind the Contractor to the prices entered on the Financial Proposal Form.

The Financial Proposal Form is used to calculate the Contractor's TOTAL PROPOSAL PRICE. Follow these instructions carefully when completing your Financial Proposal Form:

A) All Unit and Extended Prices must be clearly entered in dollars and cents, e.g., $24.15. Make your decimal points clear and distinct.

B) All Unit Prices must be the actual price per unit the State will pay for the specific item or service identified in this Solicitation and may not be contingent on any other factor or condition in any manner.

C) All calculations shall be rounded to the nearest cent, i.e., .344 shall be .34 and .345 shall be .35.

D) Any goods or services required through this Solicitation, and proposed by the vendor at **No Cost to the State,** must be clearly entered in the Unit Price, if appropriate, and Extended Price with a price of zero dollars and cents (**$0.00)**.

E) Every blank in every Financial Proposal Form shall be filled in. Any changes or corrections made to the Financial Proposal Form by the Contractor prior to submission shall be initialed and dated.

F) Except as instructed on the Financial Proposal Form, nothing shall be entered on, or attached to, the Financial Proposal Form that alters or proposes conditions or contingencies on the prices. Alterations and/or conditions may render the Proposal not reasonably susceptible of being selected for award.

G) It is imperative that the prices included on the Financial Proposal Form have been entered correctly and calculated accurately by the Contractor and that the respective total prices agree with the entries on the Financial Proposal Form. Any incorrect entries or inaccurate calculations by the Contractor will be treated as provided in COMAR 21.05.03.03E and 21.05.02.12, and may cause the Proposal to be rejected.

H All Financial Proposal prices entered below are to be fully loaded prices that include all costs/expenses associated with the provision of services as required by the Proposal. The Financial Proposal price shall include, but is not limited to, all: labor, profit/overhead, general operating, administrative, and all other expenses and costs necessary to perform the work set forth in the Solicitation. No other amounts will be paid to the Contractor. If labor rates are requested, those amounts shall be fully-loaded rates; no overtime amounts will be paid.

I) Unless indicated elsewhere in the Proposal, sample amounts used for calculations on the Financial Proposal Form are typically estimates for evaluation purposes only. Unless stated otherwise in the Proposal, the Department does not guarantee a minimum or maximum number of units or usage in the performance of this Contract.

J) Failure to adhere to any of these instructions may result in the Proposal being determined not reasonably susceptible of being selected for award.

ATTACHMENT B – FINANCIAL PROPOSAL FORM

FINANCIAL PROPOSAL FORM

The Financial Proposal Form shall contain all price information in the format specified on these pages. Complete the Financial Proposal Form only as provided in the Financial Proposal Instructions. Do not amend, alter or leave blank any items on the Financial Proposal Form. If option years are included, Contractors must submit pricing for each option year. Failure to adhere to any of these instructions may result in the Proposal being determined not reasonably susceptible of being selected for award.

See separate Excel Financial Proposal Form Attachment B.xls.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

ATTACHMENT C – NON-DISCLOSURE AGREEMENT

SRA 21-05 INTERNAL AUDIT QUALITY ASSURANCE REVIEW

THIS NON-DISCLOSURE AGREEMENT ("**THIS NON-DISCLOSURE AGREEMENT** ("Agreement") is made as of this_____day of_____, 20___, by and between the State of Maryland (the "State"), acting by and through the Maryland State Retirement Agency (the "Agency") and_____("Contractor"), Federal Tax Identification Number_____, company address_____.

RECITALS

WHEREAS, in order for the Contractor to perform the work required under the Agreement, it will be necessary for the State to provide the Contractor and the Contractor's employees and agents (collectively the "Contractor's Personnel") with access to certain confidential information (the "Confidential Information").

NOW, THEREFORE, in consideration of being given access to the Confidential Information in connection with the Agreement, and for other good and valuable consideration, the receipt and sufficiency of which the parties acknowledge, the parties do hereby agree as follows:

1. Confidential Information means any and all information provided by, or made available by, the State to the Contractor in connection with the Agreement, regardless of the form, format, or media on or in which the Confidential Information is provided, and regardless of whether any such Confidential Information is marked as such. Confidential Information includes, by way of example only, information that the Contractor views, takes notes from, copies (if the State agrees in writing to permit copying), possesses, or is otherwise provided access to, and use of, by the State in relation to the Agreement.
2. The Contractor shall not, without the State's prior written consent, copy, disclose, publish, release, transfer, disseminate, use, or allow access for any purpose or in any form, any Confidential Information provided by the State except for the sole and exclusive purpose of performing under the Agreement. The Contractor shall limit access to the Confidential Information to the Contractor's Personnel who have a demonstrable need to know such Confidential Information in order to perform under the Agreement and who have agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information. If the Contractor intends to disseminate any portion of the Confidential Information to non-employee agents who are assisting in the Contractor's performance of the Agreement, or who will otherwise have a role in performing any aspect of the Agreement, the Contractor shall first obtain the written consent of the State to any such dissemination. The State may grant, deny, or condition any such consent, as it may deem appropriate in its sole and absolute subjective discretion.
3. The Contractor hereby agrees to hold the Confidential Information in trust and in strictest confidence, to adopt or establish operating procedures and physical security measures, and to take all other measures necessary to protect the Confidential Information from inadvertent release or disclosure to unauthorized third parties, and to prevent all or any portion of the Confidential Information from falling into the public domain or into the possession of persons not bound to maintain the confidentiality of the Confidential Information.
4. The Contractor shall promptly advise the State in writing if it learns of any unauthorized use, misappropriation, or disclosure of the Confidential Information by any of the Contractor's Personnel or the Contractor's former Personnel. The Contractor shall, at its own expense, cooperate with the State in seeking injunctive or other equitable relief against any such person(s).

5. The Contractor shall, at its own expense, return to the Agency, all copies of the Confidential Information in its care, custody, control or possession upon request of the Agency, or on termination of the Agreement. The Contractor shall complete and submit ATTACHMENT C-1 when returning the Confidential Information to the Agency. At such time, the Contractor shall also permanently delete any Confidential Information stored electronically by the Contractor.

6. A breach of this Agreement by the Contractor, or by the Contractor's Personnel, shall constitute a breach of the Agreement between the Contractor and the State.

7. The Contractor acknowledges that any failure by the Contractor or the Contractor's Personnel to abide by the terms and conditions of use of the Confidential Information may cause irreparable harm to the State and that monetary damages may be inadequate to compensate the State for such breach. Accordingly, the Contractor agrees that the State may obtain an injunction to prevent the disclosure, copying or improper use of the Confidential Information. The Contractor consents to personal jurisdiction in the Maryland State Courts. The State's rights and remedies hereunder are cumulative and the State expressly reserves any and all rights, remedies, claims and actions that it may have now, or in the future, to protect the Confidential Information and/or to seek damages from the Contractor and the Contractor's Personnel for a failure to comply with the requirements of this Agreement. In the event the State suffers any losses, damages, liabilities, expenses, or costs (including, by way of example only, attorneys' fees and disbursements) that are attributable, in whole or in part to any failure by the Contractor or any of the Contractor's Personnel to comply with the requirements of this Agreement, the Contractor shall hold harmless and indemnify the State from, and against, any such losses, damages, liabilities, expenses, and/or costs.

8. The Contractor and each of the Contractor's Personnel who receive or have access to any Confidential Information shall execute a copy of an agreement substantially similar to this Agreement, and the Contractor shall provide originals of such executed Agreements to the State, upon request.

9. Data Protection and Controls

   The Contractor shall ensure satisfaction of the following requirements:

   9.1. Administrative, physical and technical safeguards shall be implemented to protect State data that are no less rigorous than accepted industry practices for information security, such as those listed below (see 10.2), and all such safeguards, including the manner in which State data is collected, accessed, used, stored, processed, disposed of and disclosed shall comply with applicable data protection and privacy laws, as well as the terms and conditions of this Contract.

   9.2. To ensure appropriate data protection safeguards are in place, at minimum, the Contractor shall implement and maintain the following controls at all times throughout the term of the Contract (the Contractor may augment this list with additional controls):

      9.2.1. Establish separate production, test, and training environments for systems supporting the services provided under this Contract and ensure that production data is not replicated in test and/or training environment(s), unless it has been previously anonymized or otherwise modified to protect the confidentiality of Sensitive Data elements.

      9.2.2. Apply hardware and software hardening procedures, as recommended by the manufacturer and according to industry best practices, to reduce the surface of vulnerability, eliminating as many security risks as possible, and document what is not feasible and/or not performed according to best practices. Any hardening practices not implemented shall be documented with a plan of action and/or compensating control. These procedures may include, but are not limited to, removal of unnecessary software, disabling or removing unnecessary services, removal of unnecessary usernames or logins, and the deactivation of unneeded features in the system configuration files.

      9.2.3. Ensure that State data is not comingled with any other data through the proper application of compartmentalization security measures.

9.2.4. Apply data encryption to protect State data, especially personal identifiable information (PII), from improper disclosure or alteration. For State data the Contractor manages or controls, data encryption should be applied to State data in transit over networks and, where possible, at rest; as well as to State data when archived for backup purposes. Encryption algorithms which are utilized for this purpose must comply with current Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules", FIPS PUB 140-2.

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

9.2.5. Enable appropriate logging parameters on systems to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information security events as recommended by the operating system and application manufacturers and information security standards, including the Information Security Policy of the State of Maryland Department of Information Technology ("Agency").

9.2.6. Retain the aforementioned logs and review them at least daily to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation, if required. The Agency shall have the right to inspect these policies and procedures, and the Contractor's performance, to confirm the effectiveness of these measures for the services being provided under this Contract.

9.2.7. Ensure system and network environments are separated by properly configured and updated firewalls to preserve the protection and isolation of State data from unauthorized access, as well as the separation of production and non-production environments.

9.2.8. Restrict network connections between trusted and untrusted networks by physically, and/or logically, isolating systems supporting the System from unsolicited and unauthenticated network traffic.

9.2.9. Review at regular intervals the aforementioned network connections, documenting and confirming the business justification for the use of all service, protocols, and ports allowed, including the rationale or compensating controls implemented for those protocols considered insecure, but necessary.

9.2.10. Establish policies and procedures to implement and maintain mechanisms for regular vulnerability testing of operating system, application, and network devices. Such testing is intended to identify outdated software versions; missing software patches; device or software misconfigurations; and to validate compliance with, or deviations from, the Contractor's security policy. The Contractor shall evaluate all identified vulnerabilities for potential adverse effect on security and integrity and remediate the vulnerability promptly, or document why remediation action is unnecessary or unsuitable. The Agency shall have the right to inspect these policies and procedures, and the performance of vulnerability testing, to confirm the effectiveness of these measures for the services being provided under this Contract.

9.2.11. Enforce strong user authentication and password control measures to minimize the opportunity for unauthorized access through compromise of the user access controls. At a minimum, the implemented measures should be consistent with the most updated and revised versions of the State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy.

9.2.12. Ensure Sensitive Data under this service is not processed, transferred, or stored outside of the United States.

9.2.13. Ensure the Contractor's Personnel shall not connect any of their own equipment to a State LAN/WAN without prior written approval by the State, which may be revoked at any time for any reason. The Contractor shall complete any necessary paperwork as directed and coordinated with the Contract Manager to obtain approval by the State to connect Contractor-owned equipment to a State LAN/WAN.

9.2.14. Ensure that anti-virus and anti-malware software is installed and maintained on all systems supporting the services provided under this Contract; that the anti-virus and anti-malware software is automatically updated; and that the software is configured to actively scan and detect threats to the system for remediation.

10. The parties further agree that:

a. This Agreement shall be governed by the laws of the State of Maryland;

b. The rights and obligations of the Contractor under this Agreement may not be assigned or delegated, by operation of law or otherwise, without the prior written consent of the State;

c. The State makes no representations or warranties as to the accuracy or completeness of any Confidential Information;

d. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement;

e. Signatures exchanged by email attachment or facsimile are effective for all purposes hereunder to the same extent as original signatures; and

f. The Recitals are not merely prefatory but are an integral part hereof.

Contractor/ Contractor's Personnel:	**Maryland State Retirement Agency**
By: _____	By: _____
Printed Name: _____	Printed Name: R. Dean Kenderdine
Title: _____	Title: Executive Director
Date: _____	Date: _____

APPROVED FOR FORM AND LEGAL SUFFICIENCY

THIS_____DAY OF_____20___.

_____
ANDREA E. YOUNG
ASSISTANT ATTORNEY GENERAL

ATTACHMENT C-1 - NON-DISCLOSURE AGREEMENT

SRA 21-05 BOARD PORTAL

CERTIFICATION TO ACCOMPANY RETURN OR DELETION OF CONFIDENTIAL INFORMATION

I AFFIRM THAT:

To the best of my knowledge, information, and belief, and upon due inquiry, I hereby certify that: (i) all Confidential Information which is the subject matter of that certain Non-Disclosure Agreement by, and between, the State of Maryland and _____ ("Contractor") dated _____, 20_____ ("Agreement") is attached hereto and is hereby returned to the State in accordance with the terms and conditions of the Agreement; and (ii) I am legally authorized to bind the Contractor to this affirmation. Any and all Confidential Information that was stored electronically by me has been permanently deleted from all of my systems or electronic storage devices where such Confidential Information may have been stored.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF, HAVING MADE DUE INQUIRY.

DATE: _____

NAME OF CONTRACTOR: _____

BY: _____
(Signature)

TITLE: _____